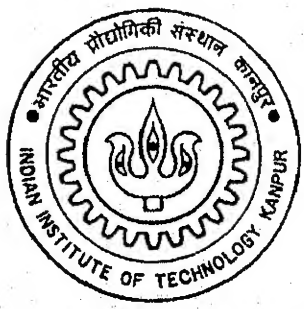
RELIABILITY ANALYSIS OF THE CAPTIVE POWER PLANT AT DUNCAN INDUSTRIES LTD. KANPUR USING PROBABILISTIC SAFETY ANALYSIS PACKAGE (PSAPACK Ver. 4.2)

by

SANTOSH KUMAR MALL

ME
1996
M
MAL
REL



DEPARTMENT OF MECHANICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY KANPUR

MARCH,1996

RELIABILITY ANALYSIS OF THE CAPTIVE POWER PLANT AT DUNCAN INDUSTRIES LTD. KANPUR USING PROBABILISTIC SAFETY ANALYSIS PACKAGE (PSAPACK Ver. 4.2)

A Thesis Submitted
In Partial Fulfillment of the Requirements
for the degree of

MASTER OF TECHNOLOGY

By

SANTOSH KUMAR MALL

to the

DEPARTMENT OF MECHANICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY, KANPUR

MARCH, 1996

9 AUG 1996
CENTRAL LIBRARY
I. I. T., KANPUR
Acc. No. A. 122029

ME-1996-M-MAL-REL

A122029

CERTIFICATE

This is to certify that the work presented in this thesis entitled " RELIABILITY ANALYSIS OF THE CAPTIVE POWER PLANT AT DUNCAN INDUSTRIES LTD. KANPUR USING PROBABILISTIC SAFETY ANALYSIS PACKAGE (PSAPACK Ver.4.2) has been carried out under my supervision and has not been submitted elsewhere for the award of degree.

K. Sri Ram

(K. Sri Ram)
Professor
Department of Mechanical Engineering
Indian Institute of Technology,
Kanpur-208016

March, 1996

ACKNOWLEDGMENTS

I am at a loss of words when expressing myself towards Professor Sri Ram, an unfailing source of inspiration in all my endeavours of last one and a half years. Be it academic or otherwise, his able guidance was indeed something rarely obtained. I am deeply indebted to him for his accepting myself under his kind supervision and providing me with an opportunity to work on reliability engineering.

My heartful of thanks are due to Mr. Sooraj Ray, Manager, Captive Power Plant, Duncan Industries Ltd., Kanpur, who allowed us the access to the CPP and then onwards enthusiastically cooperated in all our study. I am also grateful to Mr. Wilson Ferrier in this regard.

Learning to work with the PSAPACK must have been much more difficult had Dr. S. Pandimani not been there to help us. My sincere thanks to him also.

Mr. Sonal Bajaj, my friend and a partner in this study, has supported me all the way with all his efforts, while solving the problem and also at the personal level. May God bless us with a life long friendship.

I am appreciative of the way Shri Neeraj ji has constantly motivated me to higher planes all these times. I must thank Pushpesh, Parvesh, Manish, Mahendra and Avi , who have made my last two years really enjoyable.

My family has always has always stood behind me and they have every inch of the faith in my capabilities. I love them too.

CONTENTS

Chapter 1

INTRODUCTION

1.1. Overview of Reliability Analysis

Reliability is the probability of a device performing its purpose adequately for the period intended under the given operating conditions [1]. Then, consequently reliability analysis refers to studies of process or equipment failure or operability . To determine the consequences of the failure in terms of damage to property or people, a risk study could also be done. Whereas reliability analysis does improve the performance of all plants by increasing their availability , a risk study becomes mandatory when a plant failure can be hazardous e.g. a nuclear plant or a chemical plant (for instance, the Chernobyl mishap, 1986, [5] and the Bhopal gas disaster, 1984).

Reliability analysis helps one to identify the weak links in a process, in terms of unavailability. Further it also tells about the most critical sets of links, the failure of which would lead to tripping of the process. Besides one can also obtain the operational availability of a system , be it mechanical, chemical , electrical, nuclear or otherwise.

1.2. The Present Study

Though reliability engineering has mainly got confined to the realms of air craft industry and nuclear power industry but it may as well be applied to any other plant or a part of it which in fact has been the objective i.e. the reliability analysis of the Captive

Power Plant (CPP) at Duncan Industries Limited, Fertilizer Section, Panki, Kanpur. There are other (& actually bigger) power plants in the vicinity of Kanpur - Panki Power Plant of UPSEB, Auraiya Gas Project of NTPC to name a few , but a choice was made in favor of the CPP because of prior familiarity with the plant during Summer training in May-July 1993. Further the plant is relatively simpler also.

1.3. Various Available Methods

There are umpteen number of methods available for reliability analysis .The common ones being Parts Count Approach, Fault Tree Analysis (FTA) , Event Tree Analysis (ETA) , Failure Modes & Effects Analysis (FMEA) , Potential Hazards Analysis (PHA), Failure Modes effect & Critical Analysis (FMECA) etc.[6].

In the Parts Count Approach, all the components in the system and there failure probabilities are identified. Total Failure Probability is simply obtained by the addition of all of them which amounts to a pessimistic approach. Event Tree Analysis starts with considering an initiating event which may result in an accident. The second phase is to identify the accident sequences : all the possible different ways in which it may occur (they are constructed by *forward logic* i.e. one asks what happens if an event occurs). A binary analysis (success / failure) of every succeeding event after the initiating one is done. The probabilities for all such sequences are numerically estimated. In FMEA, different failure modes of a component are considered and percentages of failures in those modes are estimated. This can help in inferring whether the component is critical or not . Fair amount of working knowledge of the system is required here . In FMECA the fault and its potential effects are identified and then the existing compensation or control of them is checked about. In PHA, components are identified with their failure modes, probabilities , hazards of failure and means of early control are devised . Forward logic,

used in ETA and FMEA is often referred to as *inductive* logic, whereas the type of logic to be used in Fault Tree Analysis (discussed in next section) is *deductive*.

In the present analysis Fault Tree Analysis was resorted to ,where the system failure is modeled via a logic circuit. System hazards are frequently caused by a combination of events i.e. hardware failures along with human error and/or environmental fault events. Fault trees help to develop causal relations which can then be analyzed both quantitatively and qualitatively [5]. The advantage of using the fault tree is that it restricts the analysis only to identification of those elements & events that lead to one particular undesired failure or accident.

1.4. Fault Tree Analysis

This method entails identifying how the system may fail to function . As the word `tree' indicates , the logic diagram constructed for fault tree analysis consists of nodes and branches. The starting point in constructing a fault tree is to identify the occurrence of a single well defined undesirable event which is at the top of the tree. For a system-study , the undesirable event is obviously the non-operation of the system or an associated hazard. So working out the event combinations is aimed at which result in the occurrence of the undesirable event e.g. the accidental melting of core in a reactor at a nuclear power plant and the succeeding possibilities of a radioactive leakage as the main hazard.

The next step is to identify the probable causes of the undesirable event and relate them to the top event through appropriate gates viz. AND/OR/EX-OR etc. These causes will have further causes and they are related similarly. Such a step-by-step deductive analysis is carried out from top to down, indicating the event combinations till it finally branches into the occurrence of `basic events` i.e. events which can't be simplified further.

There can be a few events which may actually be having more explanations, (not very important to the analyst) but they are considered as basic ones for simplicity. For instance, failure of a turbine can be taken as basic event though it can attribute to many factors- casing failure / blade failure / bearing failure / nozzle failure etc. It only depends on the point of view of its utility to the person. Probabilities of the basic events can ,in general, be calculated from the empirical data or by actual operational experience .

As an example for building the fault tree and reliability analysis, the following block diagram for a simple system is considered -

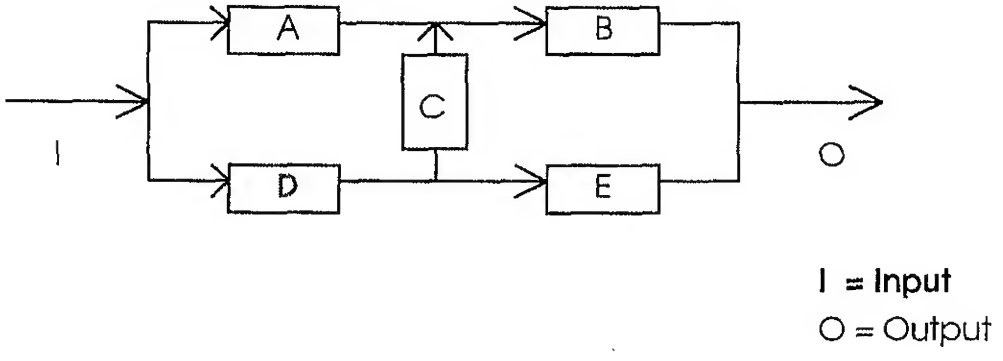


Fig. 1 Block Diagram for Example System

Here A,B,C,D,E are the components of the system. The output is not obtained in case there occurs a malfunctioning (failure) of some combination of these viz.

1. A and D or
2. B and E or
3. A, B and E or
4. A, C and E or

5. B and D .
6. A, B and D
7. B, C and D
8. B, C and E
9. A, B, C and D
10. A, B, C, D and E and so on ...

NOTE : If one thinks of the combination A, B, and D (an extra B with the first set above) then it will be found that failure of B is only causing a sort of redundancy where the system can fail with faults in A and D only. Actually, all the sets after the fifth set represent such combinations only. Thus the first five sets effectively represent the failure modes where the least number of components would be involved.

The above five sets can be represented in the form of logic gates also as in figure 2 -

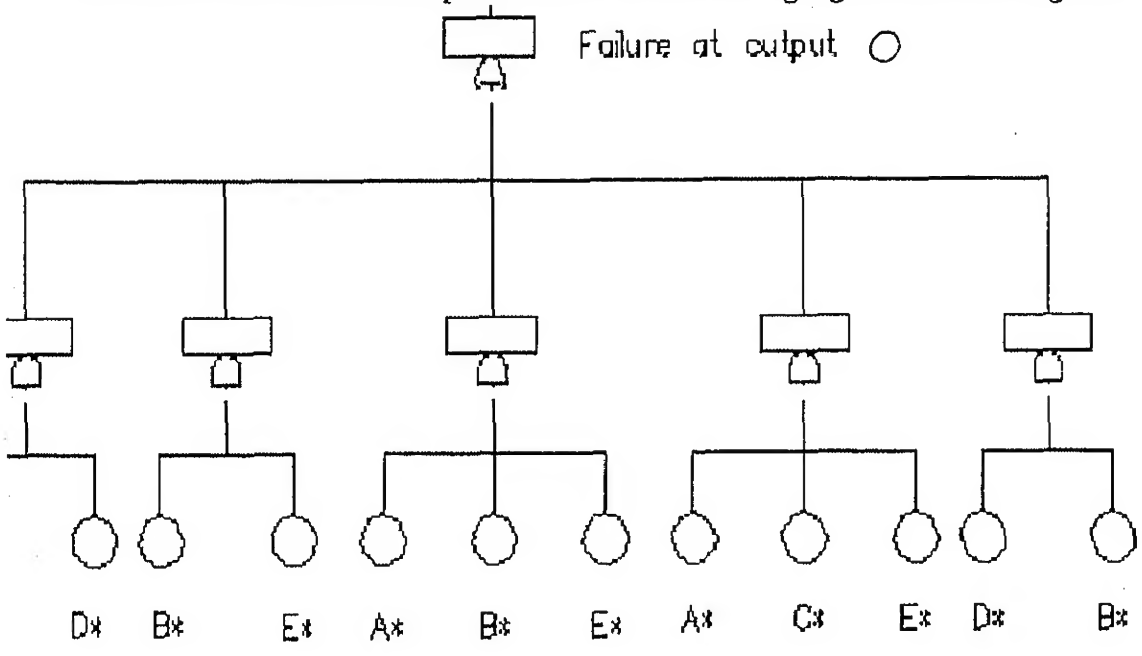


Fig. 2

* => Failure of the component

The same can be written in the boolean form as -

Failure Of Output F(O) = A*D* + B*E* + A*B*E* + A*C*E* + B*D*..... (a)

(A*,B*,C*,D*,E* represent failures)

To calculate the reliability of the system , Cut Sets enter the picture.

Cut Set

A cut set is defined as a group of elements which if they are removed from the block diagram will disconnect the input node from the output node (for a fault tree this means the set of events , the occurrence of which ensures the failure of whole system). Thus equation (a) above represents the combinations of all cut sets for the failure of the above system. It has already been noted that the terms in the above eq. can't be simplified or reduced any further.

A cut set is *minimal* when the group contains the minimum possible number of elements to cause failure (all the elements in a minimal cut set have to malfunction for the system to malfunction). So, the expressions in eq.(a) are actually the minimal cut sets for the given system failure.

If C(i) , i = 1 to 5 represent the minimal cut sets , then

C(1) = A* D*
C(2) = B* E*
C(3) = A* B* E*
C(4) = A* C* E*
C(5) = D* B*

The Probability of System Failure is given by the probability of occurrence of any of the cut sets above i.e.

Probability of System Failure F(S) = P { C(1) or C(2) or C(3) or C(4) or C(5) }

Reliability would be complimentary to the probability of failure and the former is got by subtracting the latter from unity[1] i.e.

Reliability R(S) = 1 - F(S)

Chapter 2

PROBLEM DESCRIPTION

2.1. A Brief Overview of the Plant

As already mentioned , the CPP unit of the Duncan Industries Ltd. (erstwhile Imperial Chemical Industries) is located at Panki Industrial Area , Kanpur. The main plant is designed for production of Urea, namely the brand - '*Chand Chhap*' . The CPP has the main purpose of providing about 100 to 108 Tons per hour (TPH) of Process Steam at 17.5 Kg / cm^2 pressure and saturated conditions to the Ammonia and Urea Plants. Conversion to Hydrogen and then to NH_3 by Haber's Process is done in the Ammonia Plant and this NH_3 is then used to produce Urea. The CPP has the additional advantage of producing 12 MW of electrical power (using a 12 MW turbine) which is supplied to the UPSEB for the Northern Grid.

The power plant consists of following main mechanical components - two stocker - fired furnace boilers of capacity 70 TPH of steam each, a single cylinder back pressure 12MW reaction turbine running at 3000 rpm & an attached 15000 KVA air cooled generator unit ,a boiler feed water (BFW) pump (turbine / motor driven), a set of de-superheaters, a BFW preheater, two air cooled condensers (high pressure and low pressure), an 18 ata flash drum, a water polishing unit, a few other electrically driven pumps and a very peculiar component called as ' Saturator '.(refer fig. 3)

Saturator As the name suggests, it supplies both saturated steam and water at 17.8 Kg/cm^2 pressure and 205.6^o C temperature. It acts as a cushion for the supply of saturated steam to Ammonia and Urea plants in case there is some trouble with the turbine unit and other upstream components.

STEAM FLOW DIAGRAM

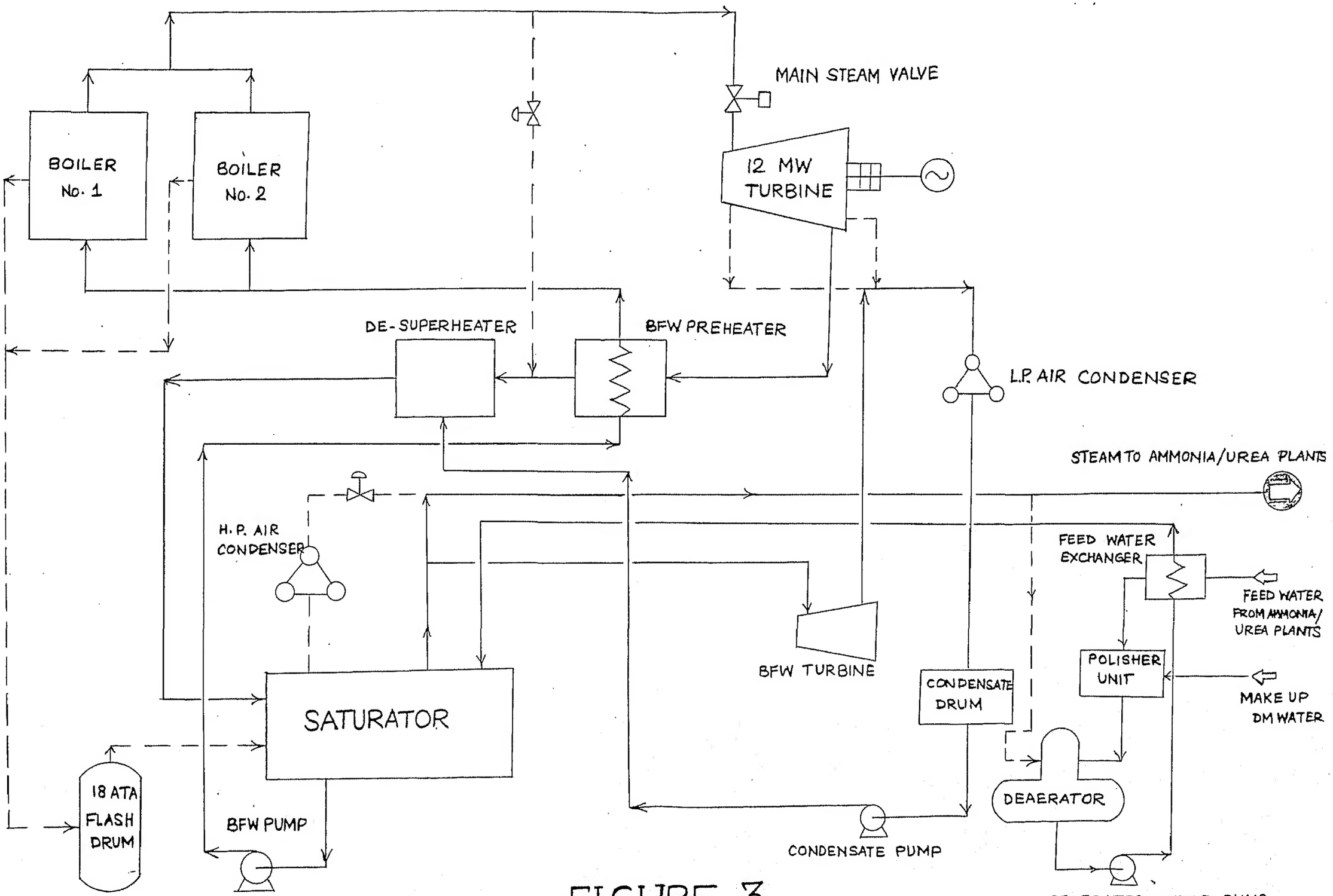


FIGURE 3

As in any actual working plant this one also brings along with the associated accessories and instrumentation. The procedure of reliability analysis has been applied only to the mechanical component failures which fall in the "Steam Flow Path". Thus only those components which are involved in a thermal balance diagram of the plant are considered for the fault tree construction. (while instrumentation and other details of a few mechanical components also have been ignored). The Steam Balance Diagram as provided by the Engineers India Ltd. to the ICI India Ltd. is the basic source for this study and it was supplemented with the discussions with the Technical Manager [7].

2.2. Details of Steam Flow Path (Refer Fig. 3)

2.2.1. Design

To start with, the feed water (for boiler) coming from the Ammonia / Urea plants which enters the water heat exchanger and then flows to the polishing unit. Here the de-mineralized make-up water from the supply i.e. the Upper Ganges Canal is also added to compensate for the losses and consumption in the cycle. Polished water is deaerated afterwards in the deaerator. This water is at pressure 17.8 Kg/cm^2 which is increased to 31 Kg/cm^2 in the deaerated water pumps and passes subsequently through the same heat exchanger to the saturator.

For the present analysis it is sufficient to assume the saturator as a black box with two incoming flow lines & two outgoing ones . The output flows saturated water and steam respectively.(Though the diagram shows a few other pipe lines also but they were found of insignificance to the failure analysis as the flow of steam was negligible though them). One input to the saturator is from the BFW supply system (described above) and the other is basically the let - down steam from the main turbine which passes through BFW preheater and the de-superheater before entering the saturator at pressure

18.5 Kg/cm^2 & temperature 205.6 $^{\circ}$ C . One of the output carries the saturated steam at 17.8 Kg/cm^2 to the main output i.e. to Ammonia / Urea plants. A part of this is taken by the BFW pump's turbine and its exhaust is condensed in low pressure air condenser, condensate from which is finally used in the de-superheater. The steam in the first output comes back as boiler feed water to the polisher unit from the Ammonia/Urea Plants after a partial consumption in the cycle. The other output goes to the boilers via BFW pump & BFW preheater.

Another input to the saturator is the steam at 18 Kg/cm^2 and temperature 206 C with a flow rate of 0.42 TPH form 18 ata flash drum. This drum is an energy conservation measure. Due to the continuous blow down needed for boiler operation a lot of heat may get wasted through the blow down water at high pressure and temperature. By flashing it from 105 Kg/cm^2 to 18 ata , steam is generated and fed to the saturator. The Company plans to utilize this steam for deaerator in the future.

When the turbo-generator unit trips or is shut off for some other purpose such as maintenance, one can still have the supply of steam to Ammonia/Urea plants through a by-pass system which consists of a valve and a high pressure condenser (which otherwise remains non-operational) and supplies to the saturator. This system is very reliable and even a hand jack is provided to operate the valve.

A few more components worth detailing are as follows -

WATER STORAGE TANK : Its a 240 m^3 capacity tank which supplies make-up water to polishing unit . In the eventuality of feed water supply cut off from mains (i.e. from Ammonia / Urea plants) it can hold the BFW supply for 2 hours and this will be the time available to manage the fault in the main supply before the boilers are forced to shut down.

BFW PUMP : It is one of the critical component in the plant when failure is concerned. The boilers can't fire unless this pump is supplying feed water to them. It is a 13 stage centrifugal pump running at an rpm of 2970 and a differential head of 1250 m.

DE AERATOR : This one is spray tray thermal type (steam is used) of capacity 40 m^3. It works at a temperature of 110 " C & pressure 1.46 Kg/cm^2. It is very reliable and seldom fails.

MAIN STEAM VALVE : Situated just before the main turbine, it is a vulnerable component with a failure rate no less than once an year.

2.2.2. Failure Mode Characteristics

The plant is considered to have failed when its basic function of providing process steam to Ammonia and Urea Plants is not accomplished, leading to a shut down in them. The failures due to power cuts are not to be considered here as the subsequent units such as the ammonia plant also do not work then. As already mentioned this main failure will be analyzed through failure of the components falling within the ambit of Steam Balance. Human operator errors are also not considered now.

Concept of Failure at a Point in a Steam Line

The CPP combines a lot many sub units which come successively in steam flow. If any point in the flow line is taken then the non-availability of steam there at the design values will be counted as a failure. There are also available (in the steam balance sheet) , few specifications for the acceptable variations (or tolerances) and they should be accounted for. The failure at that point in the flow line will have causes in terms of failures of the preceding sections and a logic can be developed which results in the construction of the Fault Tree.

For example, considering the main output as the reference point (refer fig.3A). A failure here can be caused by either

(i) A crack or other fault in the pipe line preceding to it and up to the output from the saturator , or

(ii) failure of the expansion joint at the saturator output , or

(iii) failure at the output point from the saturator.

Now this failure at the saturator outlet can be caused in following ways -

(a) failure in the saturator design itself ,or

(b) Failure at the input to the saturator, which means that any of the two inputs may fail (both of them are carrying flow rates of the same order and differ widely in thermodynamic parameters, making each of themselves a necessity for satisfactory performance of the saturator)

This way one continues further upstream the Steam Flow Path (to be analyzed in the topic of fault tree development).

Cyclic Failure Logic

As the steam flow path shows , one of the saturator output is fed to the boiler and the high pressure steam from the boilers also comes back to the saturator after due expansion in the turbine. Thus a cyclic path is constituted and this will result in a cyclic logic as well with the same component being considered twice in the same branch of the fault tree. Obviously it needs to be broken at a suitable location. The boiler units have been taken at the base of the failure analysis i.e. the input lines to the boilers are not considered for failure analysis (though all the components in that line have already been taken into cognizance)

CENTRAL LIBRARY
I. I. T., KANPUR
A. 122029

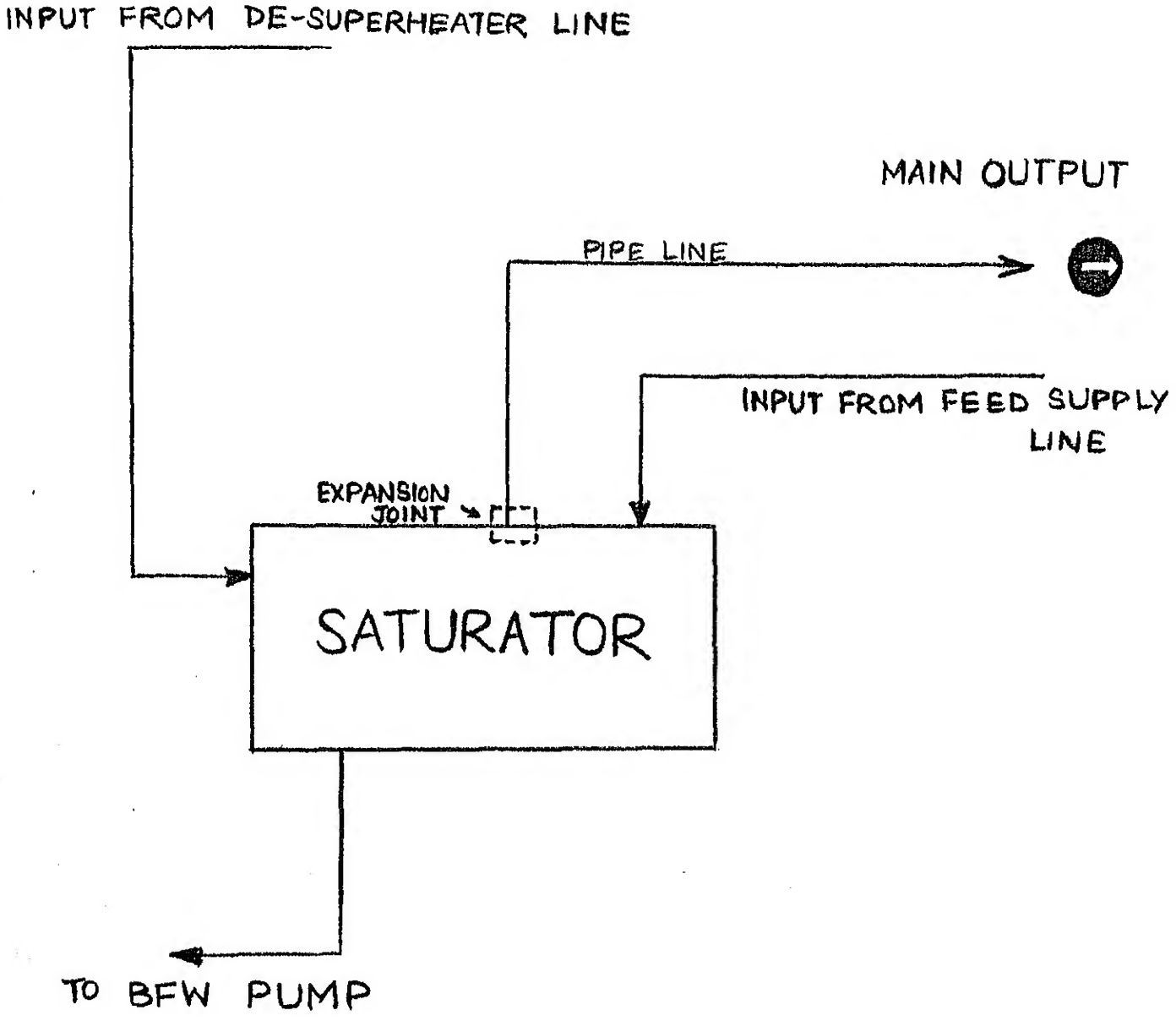


FIG. 3A FAILURE AT MAIN OUTPUT & SATURATOR

Design Faults

By this is meant the non-functioning of the design of various components such as turbines, pumps, condensers, saturator, heat exchangers etc. They have been taken as basic events of failure and more details of their failure haven't been analyzed because further sub-division of their working principles appeared redundant for this study. Therefore they have been accorded the status of diamond shaped basic events in the fault tree.

2.3. Developing the Fault Tree

2.3.1. Break Up (Refer Fig . 4)

The top most resultant event is the non availability of steam at the plant outlet. As explained in 2.2.2 above the top event would be followed by an OR gate with inputs of two basic events (pipe line and expansion joint failure and a resultant event (i.e. a rectangular box) depicting failure of saturator system supply. This resultant event would be followed by an OR gate once again which has three inputs- one basic event of saturator failure and two resultant events which are the failures in the two supply lines to the saturator i.e. *De - superheater line & Feed Supply line* (from polishing unit) , to be considered separately .

It needs to be noted here that this plant involves steam flow at high temperature (about 200 ^{o}C) and thus almost all the pipe line ends will have expansion joints connecting them to other components. Pipe line fault is a basic event possible for all the piping sub-sections considered and similarly is the expansion joint failure. Thus it is found that these two basic events have become the most frequent ones in the tree and they appear nearly in all the branches (Here onwards, description about them in every step of the fault tree has been avoided).

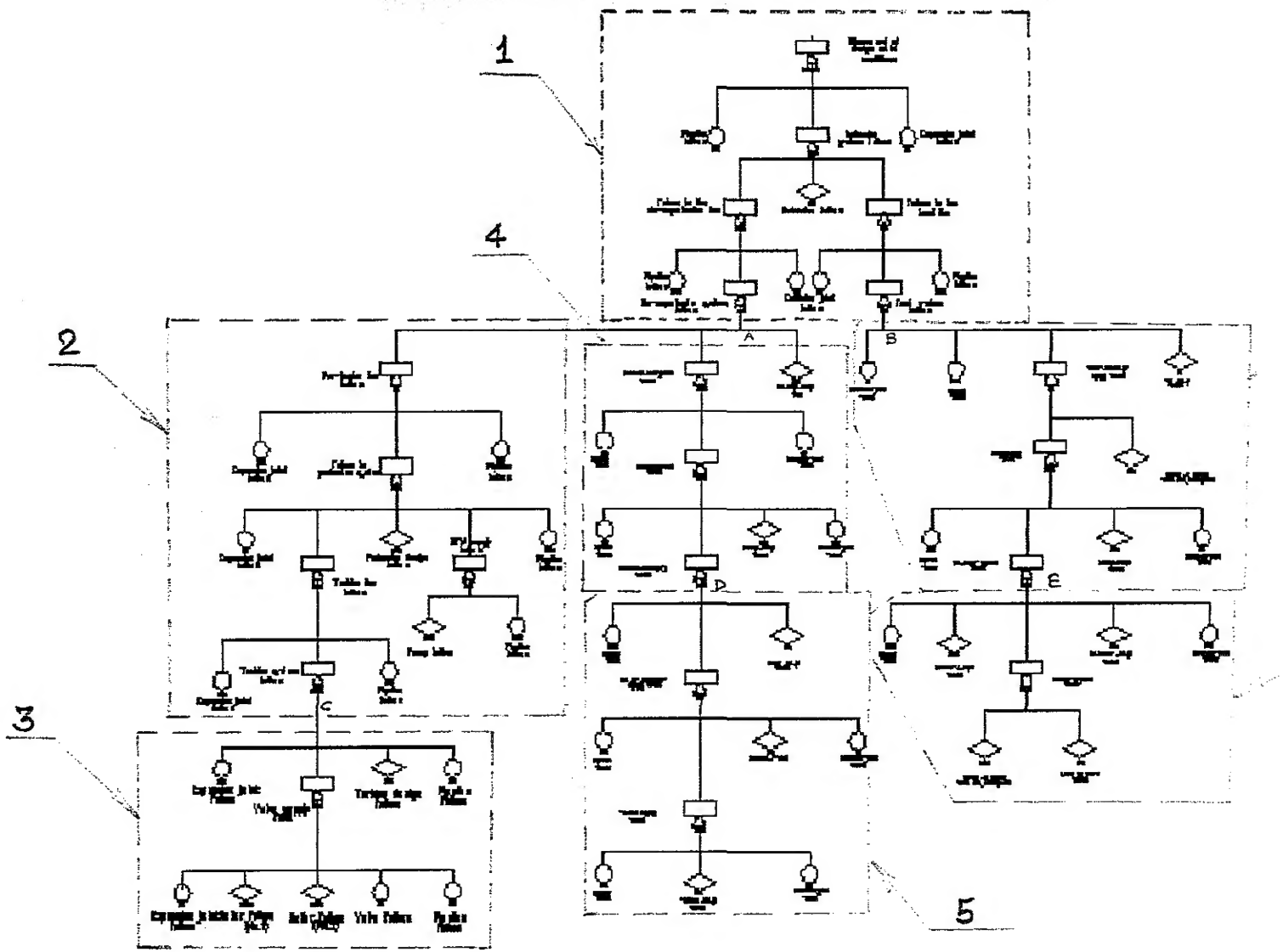


Fig. 4 Fault tree for the CPP

(enlarged on the following fig. 4(1) – 4(7))

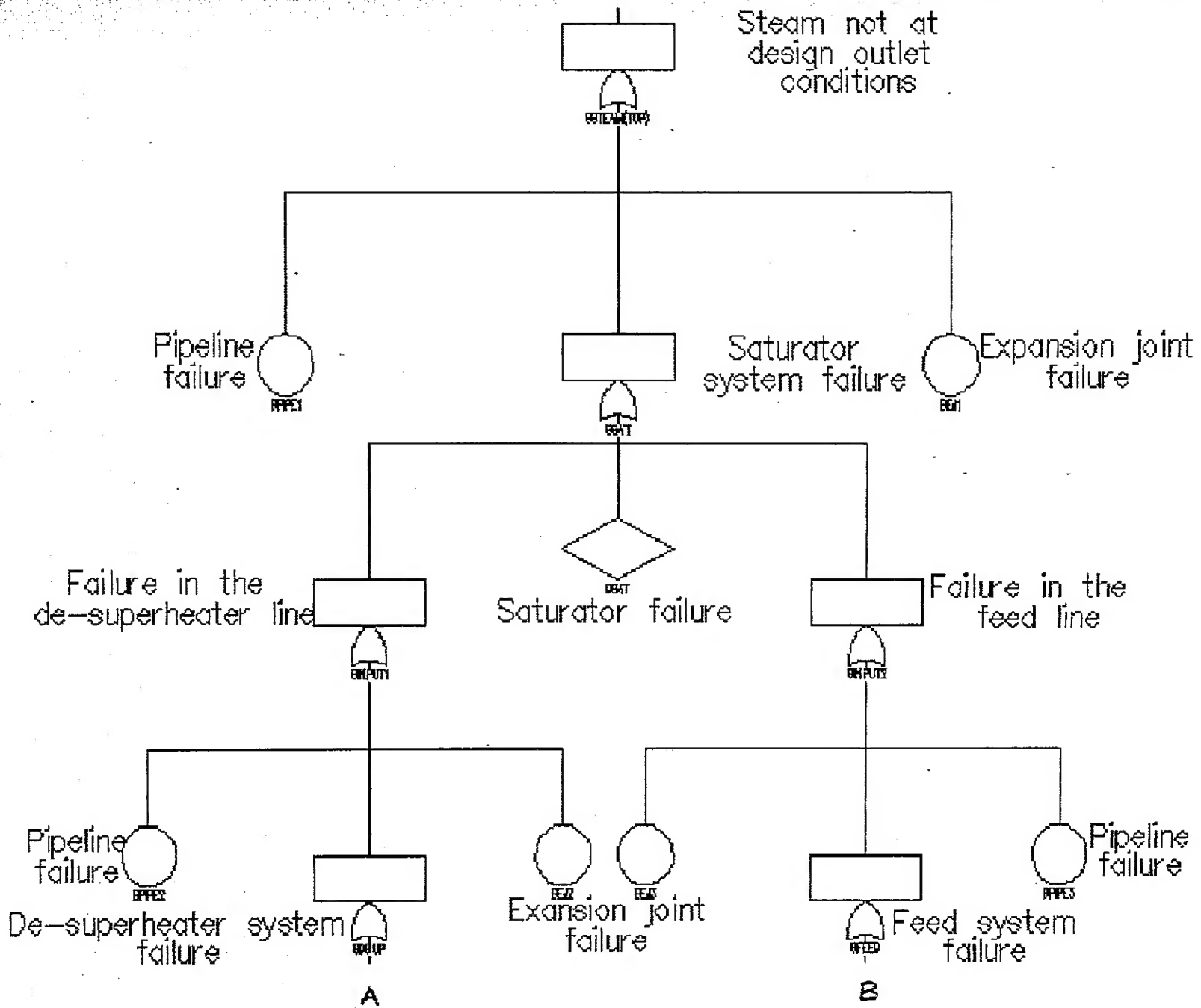

Steam not at design outlet conditions
Pipeline failure
Saturator system failure
Expansion joint failure
Failure in the de-superheater line
Saturator failure
Failure in the feed line
Pipeline failure
De-superheater system failure
Exansion joint failure
Feed system failure
Pipeline failure
A
B

Fig. 4 (1)

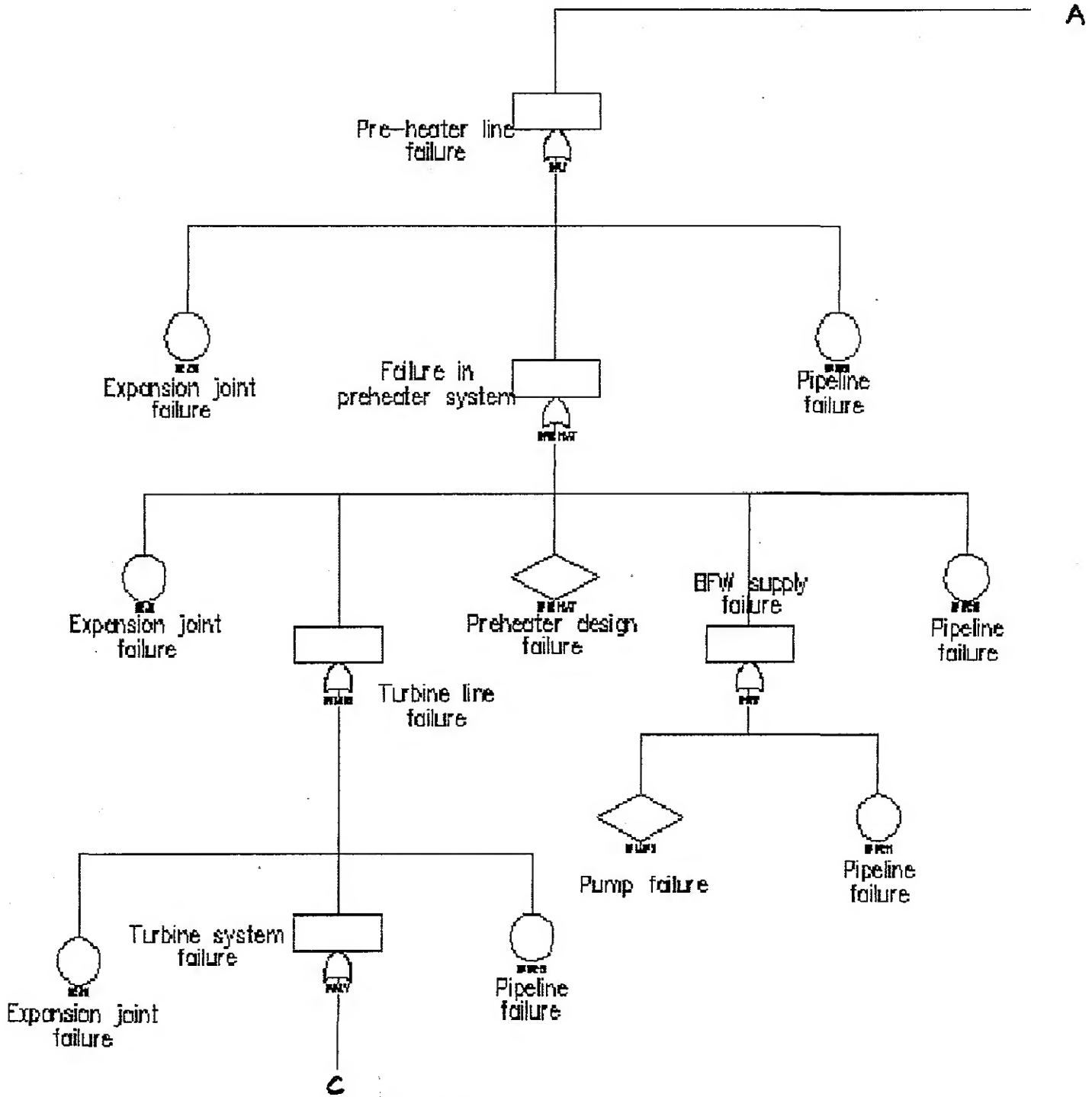

A
Pre-heater line failure
Expansion joint failure
Failure in preheater system
Pipeline failure
Expansion joint failure
Turbine line failure
Preheater design failure
BFW supply failure
Pipeline failure
Pump failure
Pipeline failure
Turbine system failure
Expansion joint failure
Pipeline failure
C

Fig 4.(2)

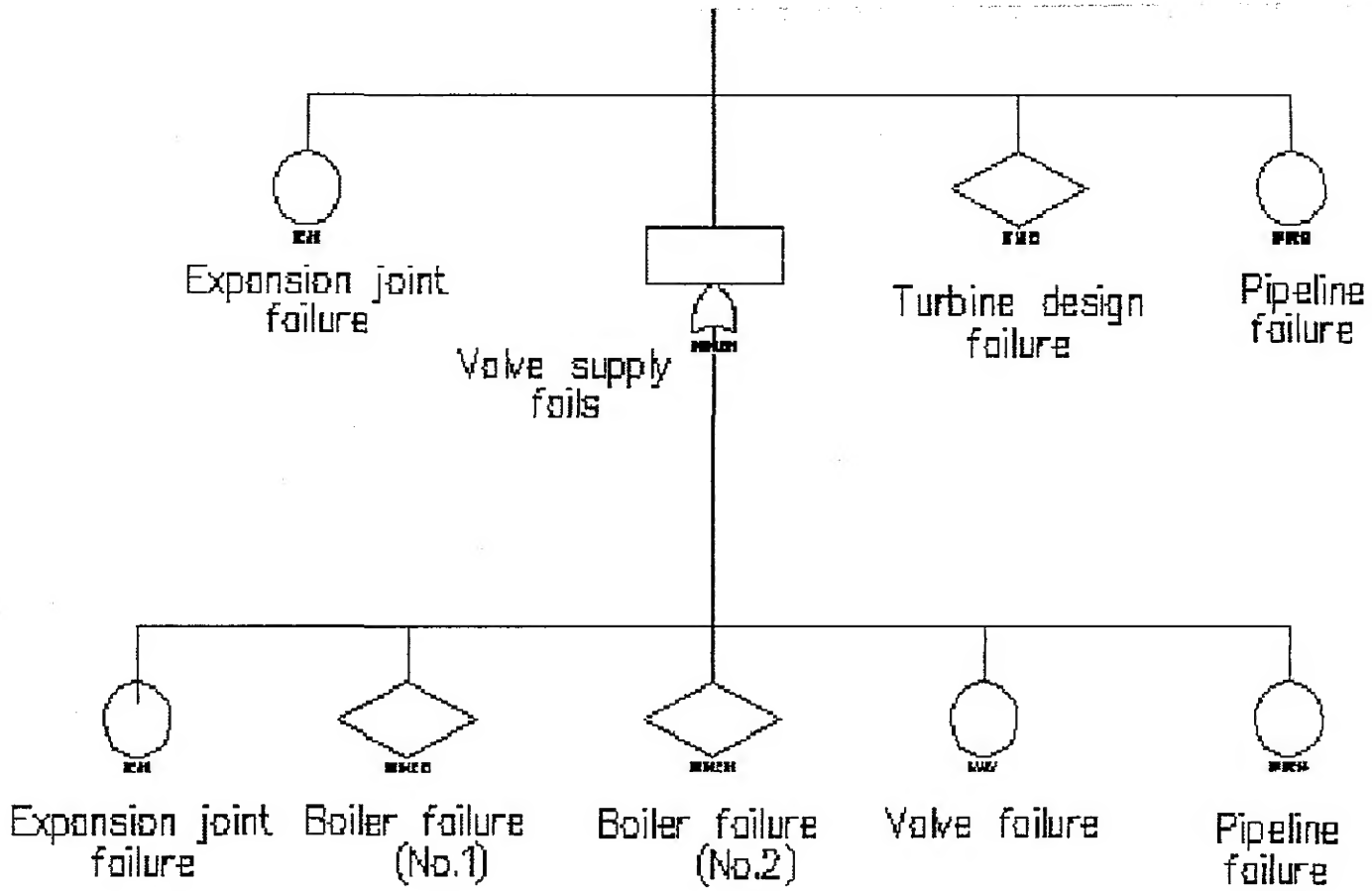

Expansion joint failure
Valve supply fails
Turbine design failure
Pipeline failure
Expansion joint failure
Boiler failure (No.1)
Boiler failure (No.2)
Valve failure
Pipeline failure

Fig. 4 (3)

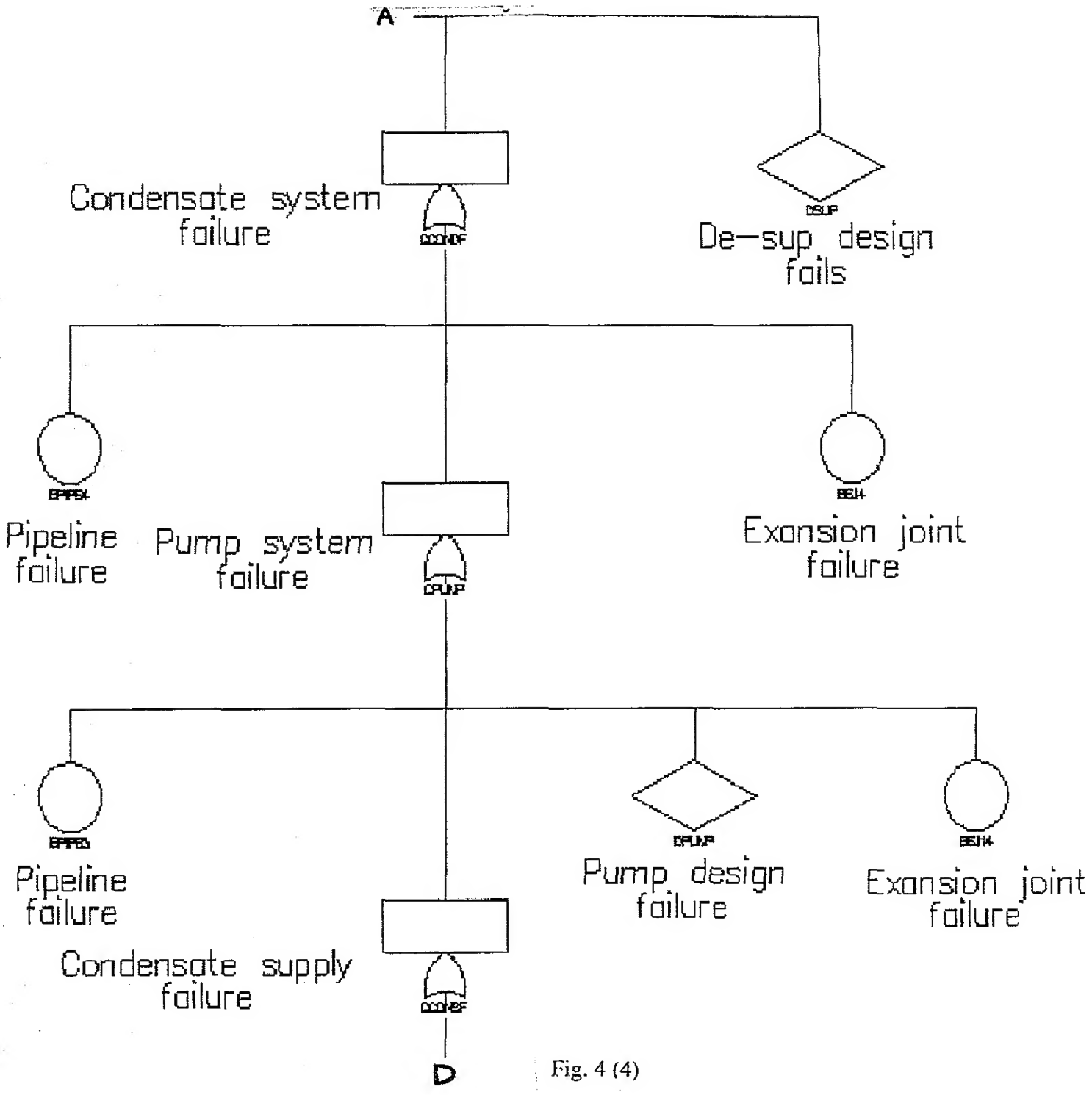

A
Condensate system failure
De-sup design fails
Pipeline failure
Pump system failure
Exansion joint failure
Pipeline failure
Pump design failure
Exansion joint failure
Condensate supply failure
D

Fig. 4 (4)

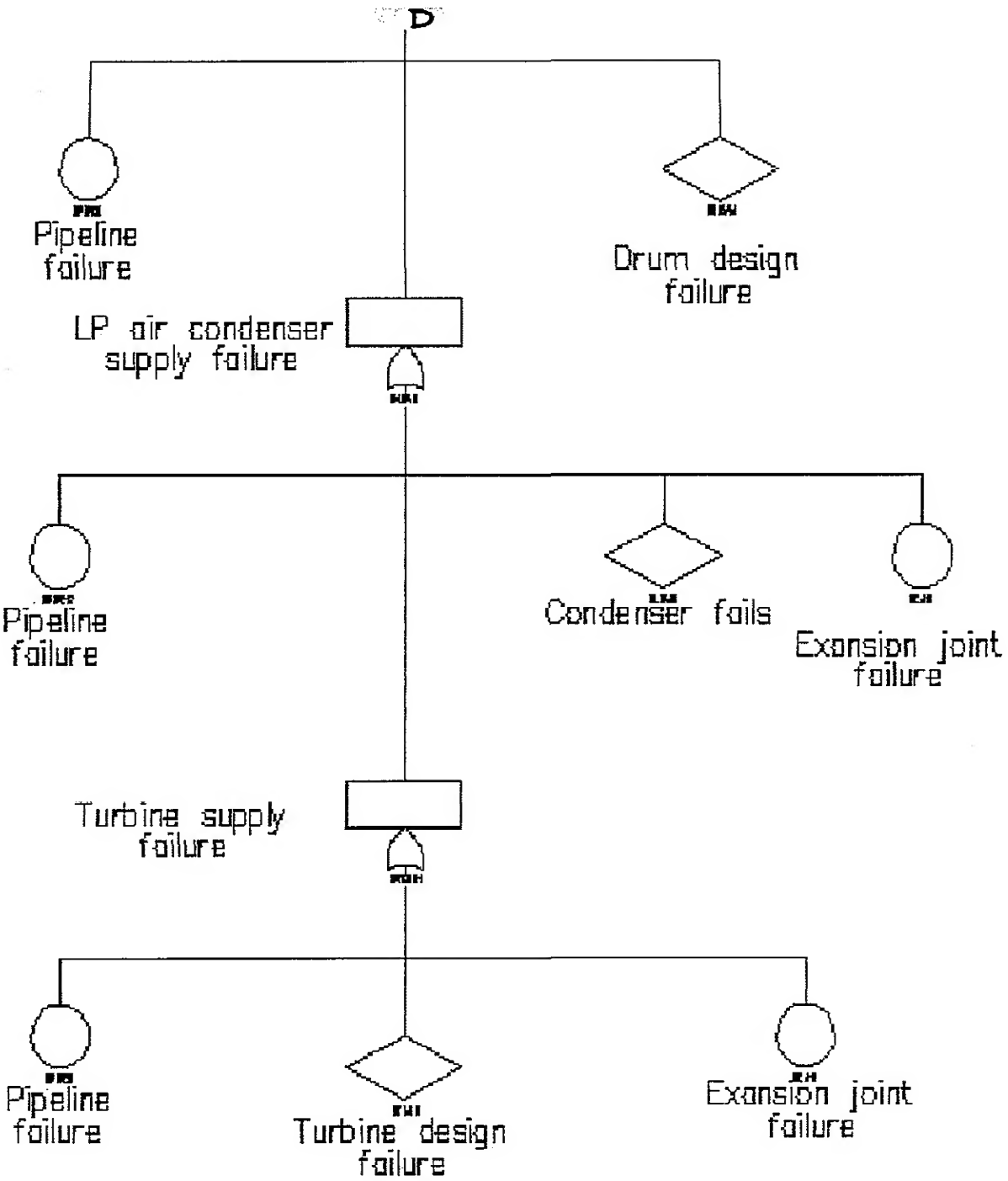

D
Pipeline failure
Drum design failure
LP air condenser supply failure
Pipeline failure
Condenser fails
Exansion joint failure
Turbine supply failure
Pipeline failure
Turbine design failure
Exansion joint failure

Fig. 4 (5)

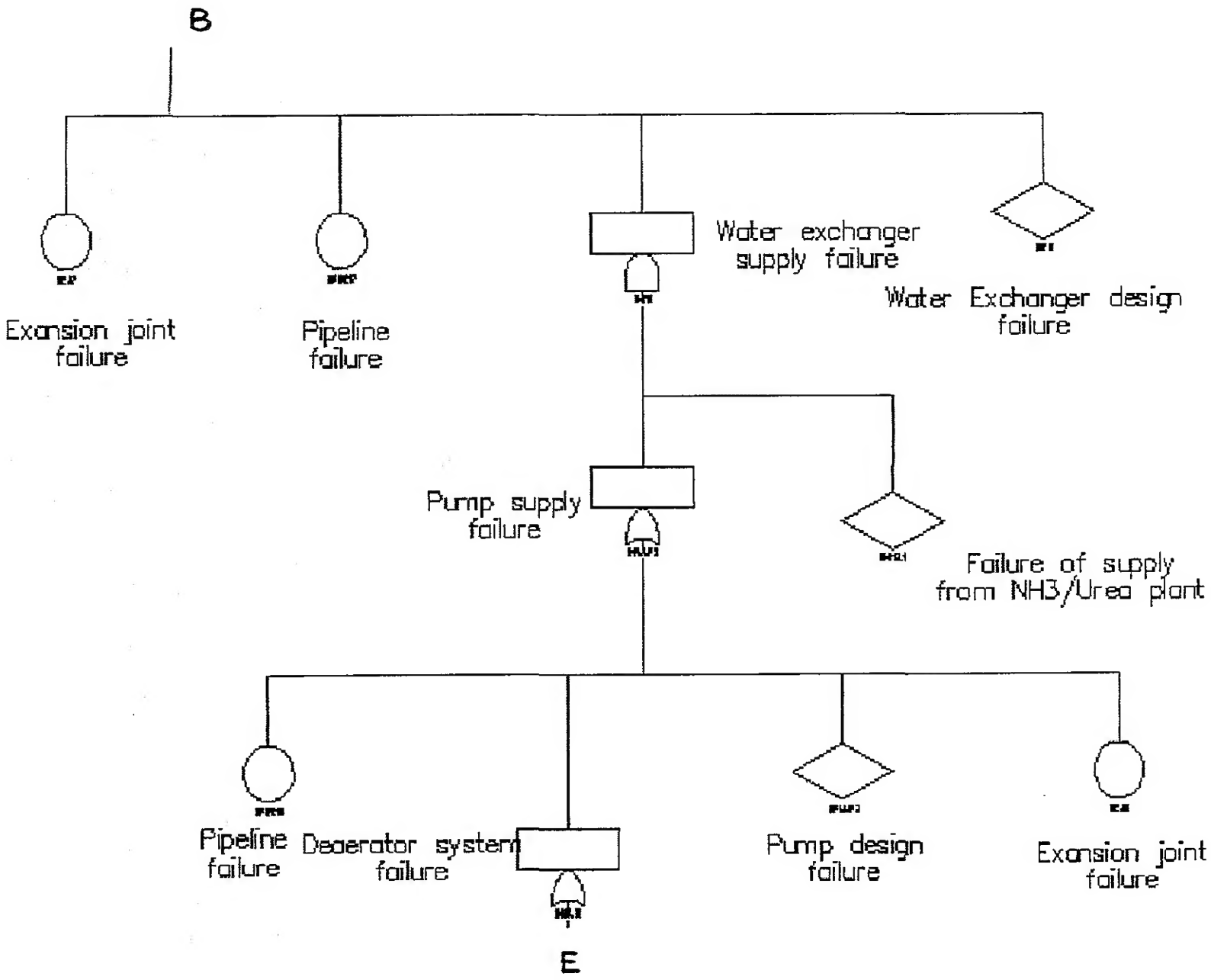

B
Exansion joint failure
Pipeline failure
Water exchanger supply failure
Water Exchanger design failure
Pump supply failure
Failure of supply from NH3/Urea plant
Pipeline failure
Deaerator system failure
Pump design failure
Exansion joint failure
E

Fig. 4 (6)

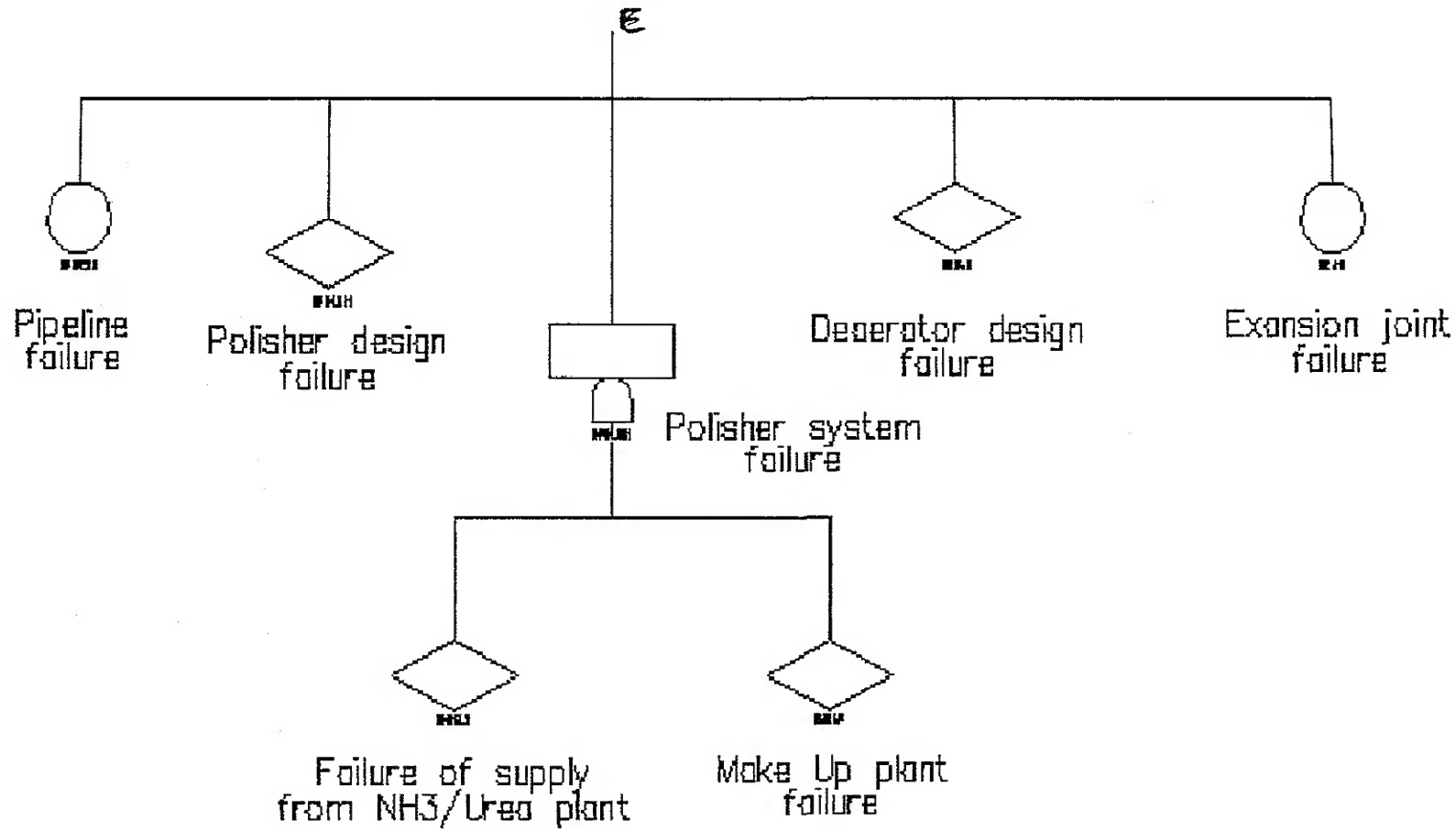

E
Pipeline failure
Polisher design failure
Deaerator design failure
Exansion joint failure
Polisher system failure
Failure of supply from NH3/Urea plant
Make Up plant failure

Fig. 4 (7)

(A) De - superheater Line Failure

This involves a fault either in the de-superheater design or in the two inputs to it viz. the *Preheater output line or the Condensate supply line*, hence an OR gate at this level is used .

Preheater Line Failure

The preheater has two inputs, the turbine output line and BFW Supply line with almost the same flow rates and different temperatures . Thus a failure of any one of them is sufficient to cause a great variance from the desired at the preheater output. So an OR gate represents this system. Preheater design failure is the other basic event connected to this gate.

The BFW supply line involves only the BFW pump and a piping section in an OR gate combination. (one needs to stop here because a further explanation of failure at the pump input will involve saturator failure and thus cyclic logic)

The turbine output can fail when either of the turbine design or the supply from the main steam valve (MSV) fail . Valve supply failure involves a fault in the valve or the boiler supply itself failing which is a basic event at the bottom of the tree.

Condensate Supply Line Failure

The condensate from the BFW pump's turbine and main turbine is pumped up at the condensate pumps. This supply line involves a low pressure air condenser , a condensate drum, pumps and various piping sub-sections . A failure in any one of the above means condensate supply failure to the de-superheater. So they are all connected via a few OR gates in various branches to account for all the piping sections & expansion joints and also for clarity.

(B) Feed Supply Line Failure

BFW to the saturator is coming from the Feed water / deaerated water exchanger . This can go off either when the heat exchanger's design fails or its supply line goes wrong. This resultant event of supply failure shall occur only when both the inputs fail viz. the BFW line from Ammonia plant (taken as basic event) and the line from deaerated water pump, a resultant event (so an AND gate connects the two). The latter is a result of either the failure of the deaerated water pump design itself or of its supply which comes from the deaerator (a resultant event). Now, deaerator output failure comprises of a fault in its design or a fault in the input to it. But the input failure means a failure of both the two supplies, namely, the Ammonia/Urea plant feed water line (a basic event) and the Make Up supply (a basic event)(hence an AND gate connecting the two).

2.3.2. Approximations and Justifications

The steam demand varies from about 100 to 108 TPH and all the main steam lines which affect the availability of the plant also carry a similar flow rate of steam / feed water. Therefore it can be safely chosen to ignore the flow lines with the flow rates less than about 2 TPH and a majority of the approximations revolve around this idea. At some places this concept has helped in simplifying the tree and also avoiding the loop in failure logic. They can be elaborated as following -

(i) HP Air Condenser & By-Pass Line

This condenser is put into service only when there is a major breakdown in the main turbine section and the high pressure steam is by-passed to the saturator for the sole purpose of getting process steam in such an emergency. Then it can be viewed as a

stand-by arrangement (of course not to generate power) for the main turbine failure. Since time dependent modes of failure analysis haven't been considered , this section has been omitted from the tree.

(ii) 18 Ata Flash Drum

It entails a flow rate merely of 0.4 TPH and supplies it to the saturator with only a very small effect on heat balance. A failure here would minutely affect the performance of the saturator. Thus the flash drum seems not to affect the overall plant availability much and can be ignored.

(iii) Let Down System

This flow line carries about 2 TPH steam at 455 " C temperature and 18.5 Kg/cm^2 pressure. The enthalpy at these conditions is 803.2 Kcal/Kg (=> net flow enthalpy = 4016 Mcal per hour) . This line adds to the preheater output which means 124.5 TPH of steam at 231° C and same pressure as above which implies an enthalpy value of 683.3 Kcal/Kg and a net flow enthalpy of 85071 Kcal/hr . This is about 21 times more than the first line. So a failure at the let down valve can be easily met with by slight adjustments in the turbine line (the operational experience at the factory) . So this line was not considered for failure analysis.

(iv) Partial Outlet of the Main Turbine

Though at a high temperature of about 350 ° C ,this section flows only 0.6 TPH of steam at pressure 1.5 Kg/cm^2 to the low pressure condenser and involves only a small pipe line section as the failure component and hence can be easily ignored.

(v) Steam Line to the Deaerator

The deaerator is getting its steam from the main supply line just before the plant outlet point and the amount is 1.52 TPH (saturated main supply conditions). Now the failure of this steam supply essentially amounts to the failure of the main supply of steam which is the topmost event of the fault tree and so can't be considered as it would mean a logical loop. Thus only a small piping section is left and it could be ignored.

Chapter 3

THE PACKAGE USED FOR ANALYSIS - PSAPACK

After the construction of the fault tree , it needs to be analyzed for minimal cut sets and thus get the idea about plant unavailability figure. Manual analysis and calculations could be performed for simple trees, basically those which extend into 4 or 5 steps. This is a much bigger sample and actually, in practice, there are very large trees once one considers all the minute details of a plant (here only the steam balance part has been taken). A computer program was needed to perform the calculations.

Several computational codes have been so far developed to achieve this. MOCUS [2] and F-TAP [3] are among the most widely used . MOCUS algorithm is an example of top to down search. F-TAP follows the reverse approach of bottom to up search and is capable of handling larger trees. There is the software - Probabilistic Safety Analysis Package version 4.2 (PSAPACK) on the personal computers of the Nuclear Engineering & Technology laboratory , which can perform the cut set analysis and compute the average unavailability besides several other functions. It had been developed in 1993 by the International Atomic Energy Agency (IAEA) in cooperation with its Member States. The principal developers of PSAPACK are A. Bojiadiev of Risk Engineering Ltd. Bulgaria and H. Vallerga of Commision Nacional de Energia Atomica, Argentina [4].

PSAPACK is an integrated fault / event tree package with capabilities for user friendly recalculations and easy interrogations of results [4]. There are two levels of processing in the package -

3.1. Levels

Level A - Decision Maker

It is for operational safety management. It works on the basis of minimal cut sets generated in level B and updates the plant status considering specific components out-of-service and forecast the impact on the top most event of the tree viz. core melt in a nuclear power plant or the failure of process steam supply at our plant.

Level B - PSA Analyst

It contains the features needed for performing the reliability analysis / probabilistic safety analysis. They include : fault tree editor (graphic & text) ; fault tree analyzer (SETS code) ; event tree construction and analysis (graphic & text) ; accident sequence boolean reduction and quantification ; reliability data base (generic data , unavailability evaluation, component attributes) ; utilities (help functions, on line code manual and PSA procedures guide).

The various tools of PSA are contained in the various modules of the package -

3.2. Modules

RDB

Reliability Data Base module is used for the management of reliability data . This module can create a user defined data base or retrieve data from the IAEA Generic Reliability Data Base (GRDB). RDBs for components, human actions, initiating events and attributes of components can be developed.

Component unavailability can be calculated based on the data base reliability parameters using 10 types of predefined reliability modules which are -

TYPE		DESCRIPTION
0	=	Quantification not performed
1	=	Stand-by test component
2	=	On-line non-repair component
3	=	Stand-by nontest component
4	=	Stand-by monitored component
5	=	On-line monitored component
6	=	Stand-by (monitored) / Oper. (non repair) component
7	=	Stand-by (test) / Oper. (monitored) component
8	=	Stand-by (test) / Oper. (non repair) component
9	=	Constant Unavailability = Failure per demand

A constant failure rate (central part of the bath tub curve, discussed in the next chapter) has been assumed and so type 9 is the main concern.

FTE

The Fault Tree Editor module edits and manages fault trees in the text format (sequential specification of fault tree by giving code names to the gates and events) . It automatically verifies the fault tree logic and also checks about the definition of all the components in the RDB modules (if any of the components of a fault tree is not described in the RDB module also then it gives an error message while saving the tree).

FTA

The Fault Tree Analyzer module reduces the fault trees and generates the minimal cut sets (MCS), which are stored in the MCS library. There are many options available for doing this and they can be selected based upon the memory requirement of each and thus the compatibility with the computer (e.g. F-TAP requires a minimum of 450 KB of memory space where as the SETS code, running on a 386 PC with Math Coprocessor, needs atleast 2 MB memory). Each cut set involves a probability of failure and if that comes out to be too low , the program can ignore the cut set altogether. This quantifiable

control on the cut sets is performed using ' truncation cut-off probability' which can be specified by the user depending upon the capabilities of the computer.

VIEW

This is for quantification. All minimal cut sets are stored in the specific libraries for the fault trees, super components (an event which is a tree in itself is defined as a super component) and sequences. The VIEW module recalculates the point estimates in the various libraries each time it is used. It is basically this module which provides us with the final results in a tabular form.

ETED

The Event Tree EDitor module edits and manages the event trees in text format. Event trees can be created in two ways - In text format inputting "0","1","2","-" as coding system or developing the logic accident sequences based on user specified dependencies between event tree headings and defining success criteria for sequences.

BOOLRED

The BOOLean REDuction module generates minimum cut sets from sequences combining the minimum cut sets (generated by FTA module) using a boolean algorithm. BOOLRED provides an automatic handling of success paths and it is possible to truncate the sequence minimal cut sets by probability or order.

FEP

This is the Fault tree, Event tree and Piping & Instrumentation Diagram Editor which is a program having all the common graphical tools needed for performing risk assessment. Fault trees, event trees and piping & instrumentation diagram can be all built graphically and edited thereafter through this module. Where as graphical fault trees and event trees, generated here can be both directly accessed from the respective text editing

modules viz. FTE & ETE, vice versa is true only for ETE , not FTE. These drawings can be documented and printed whenever needed.

STATUS

This can reevaluate a plant status given a specific plant configuration. Updating of the current status is done by selection of components out of service or by introducing human errors at a given time. In this module it is possible to change the data of an existing plant status selecting the basic events according to systems, initiating event, event code or attributes.

The PSAPACK has a few global constraints on fault trees, gate labels, gate logic, component labels and component parameters and they should be adhered to for smooth running of the program e.g. more than 20 inputs to any gate in a graphic fault tree causes problems when transferring to text fault tree data base and this can be easily avoided by adding steps (more gates) to the fault tree.

Although the program is user friendly with the most of it being menu driven and has on-line help facility, the manual provided along with is of great value. Solving a few practice problems helped in getting familiar with the program towards the main problem.. Next thing was to search for the reliability data - taken in the following chapter.

Chapter 4

RELIABILITY DATA BASE

4.1. The Model

Reliability factor , for a given set of components under test , can be defined as the ratio of survivors at any given time to the total initial population. As the test proceeds , more components fail, with the result that the reliability factor decreases progressively [1]. Such reliability factors can also be called as *probabilities of survival.* Now probabilities of survival are simply obtained from subtracting the probabilities of failure form unity as survival and failure are complimentary events.

As has been discussed in chapter 1

Reliability of System = 1 - Probability of System Failure

Failure probability for a system is easily calculated by the method of cut sets. This requires the probability of failure for the most basic events. This is linked with experimental or field failure data. Failure data comprises of failure density (for a given interval of time), failure rate reliability and probability of failure. These parameters are interrelated.

The behavioral characteristics exhibited by separate classes of components are different. Different mathematical models are there to represent them viz. Constant Hazard, Linearly Increasing Hazard & Weibull model. Where as the constant hazard model assumes a failure rate constant with time (corresponding to the middle zone of the 'bath tub' curve, refer fig. 5), linearly increasing hazard assumes that wear or deterioration is

increasing the hazard rate linearly. The Weibull model takes care of non linearity of the variation of hazard rate with time.

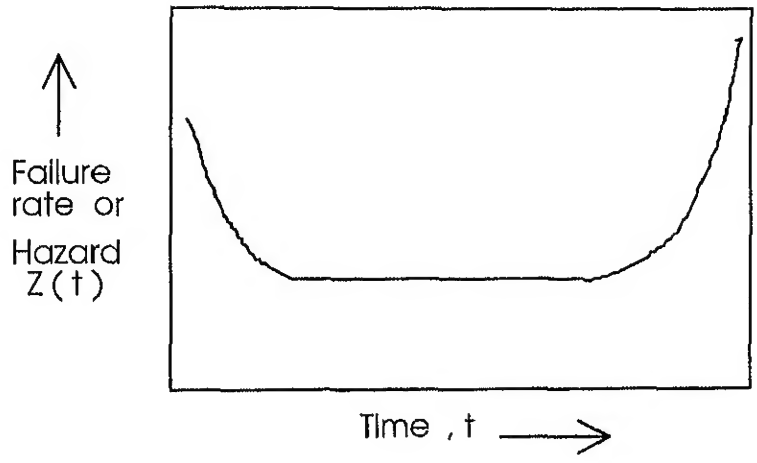


Fig. 5 The Bath Tub Curve

The Constant Hazard model has been taken for this study and therefore the reliability data needed for the basic events would be their failure rates in a given unit of time, which has been taken as an hour.

4.2. Sources of Data

As per the discussions with the technical manager [7], the components can be classified in two categories - those which have high frequency of failures and others having very small failure rates. Boilers, BFW pump, saturator, main steam valve can be taken in the first. Components such as piping sections, expansion joints, condensers can be a part of second type. Broadly, this categorization also holds good when one looks for the sources of data i.e. from actual plant experience at CPP and the generic data base stored in PSAPACK, respectively. The generic data base has been considered first.

4.2.1. Generic Data in the Package

This data base from IAEA has been compiled from a lot many studies and reports, chiefly the WASH 1400,1974; German Risk Study, 1979; IEEE Standard 500,1984; NUREG ,1983 -86; Shoreham PRA, GE data and a few others [8]. This is quite an exhaustive coverage and contains information and reliability data about various mechanical components such as piping, heat exchangers, control rods, pumps, valves, air handling equipments, instrumentation and control equipments besides various electrical components. The information about the components includes - failure rates , test intervals, mission time, repair time, probability of human error, test period, failure modes and other specifications about the item such as material, size etc.

The IAEA data has been collected for the following set of components (failure rate per hour) -

COMPONENT	GRDB Code	FAILURE RATE
Expansion Joints	FEATH	5.90×10^{-8}
Piping Sections	FSAAE	9.40×10^{-6}
Condensate Pump	PMBRP	1.80×10^{-5}
Deaerated Water Pump	PMBRP	1.80×10^{-5}
Preheater	HXVAF	1.14×10^{-5}
Drum	HXA6B	1.14×10^{-5}

Although the fault tree contains a large number of basic events for pipe line & expansion joint failure which are of different specifications about their sizes and thus there can be small variations in their probabilities of failure but they have been taken as general pipe line failure and expansion joint failure because of two reasons - firstly theirs having very small failure rates , small variations don't matter much and secondly due to the insufficient details available from the drawing .

4.2.2. Data from Duncan Industries Ltd.

There were a few components which were not available in the generic data base e.g. saturator, condenser, boiler, polisher etc. The events such as failure of BFW supply from Ammonia plant are specific to this plant only. Also some components are actually having high failure rates compared to those in the generic data. In all such cases resort to the information provided by the Technical Manager [7] for failure data has been made. The number of times the components did fail in preceding 13 odd years were told about. From this was made an average estimate about the probability of failure per year and thus the failure rate per hour. The components and their failure rates are as following -

COMPONENT	FAILURE INSTANCE	FAILURE RATE (per hour)
Saturator	twice in 10 years	2.28×10^{-5}
One Boiler	twice per year	2.28×10^{-4}
BFW pump	once per year	1.14×10^{-4}
Main steam valve	once per year	1.14×10^{-4}
Deaerator	once per 12 years	9.40×10^{-6}
LP air condenser	once per 10 years	1.14×10^{-5}
Turbines	once per 14 months	1.00×10^{-4}
Polisher unit	once per 10 years	1.14×10^{-5}
Water exchanger	once per 10 years	1.14×10^{-5}
Ammonia plant supply	once per 10 years	1.14×10^{-5}
Make up supply	once per 12 years	9.40×10^{-6}
De-superheater	once per 12 years	9.40×10^{-6}

Chapter 5

RESULTS

The graphic fault tree shows the events and gates with detailed text descriptions along with but the text editor and also the RDB module can't take in big names for the events etc. Codes were applied for their names. The fault tree as it appears in the tabular text format is shown on the following page. Descriptions for the codes have been described here -

Gate Name	Description
GSTEAM (TOP)	Failure of steam supply at plant outlet
GSAT	Failure at saturator outlet point
GINPUT1	Failure in de-superheater line
GINPUT2	Failure in feed line
GDSUP	Failure at de-super heater outlet
GFEED	Failure at feed system outlet
GCONDF	Condensate system supply fails
GWX	Water exchanger supply fails
GPLF	Preheater line fails
GPUMP2	Deaerated water pump supply line failure
GPUMP	Condensate pump supply line fails
GPREHEAT	Failure at the preheater output
GBFW	BFW supply to the preheater fails
GDEAIR	Failure at the deaerator outlet
GMTURB	Failure in main turbine line
GCONSF	Failure of supply of LP condensate
GPOLISH	Input failure at the polisher unit
GTURBOUT	Failure at the main turbine outlet point
GLPAIR	Failure at the outlet of LP air condenser
GBOILER	Failure at the combined outlet of the boilers
GPTURB	BFW pump's turbine outlet failure

GATE	TYPE	INPUT 1	INPUT 2	INPUT 3	INPUT 4	INPUT 5
GSTEAM(TOP)	OR	BPIPE1	GSAT	BEJ1		
GSAT	OR	DSAT	GINPUT2	GINPUT1		
GINPUT2	OR	BEJ3	BPIPE3	GFEED		
GINPUT1	OR	BPIPE2	BEJ2		GDSUP	
GFEED	OR	DWX	BPIPE17	BEJ7	GWX	
GDSUP	OR	GCONDF	DSUP	GPLF		
GCONDF	OR	BEJ4	BPIPE4	GPUMP		
GWX	AND	GPUMP2	DNH3.1			
GPLF	OR	BEJ20	BPIPE9	GPREHEAT		
GPUMP2	OR	BEJ9	DPUMP3	BPIPE19	GDEAIR	
GPUMP	OR	DPUMP	BEJ14	BPIPE5	GCONSF	
GPREHEAT	OR	BEJ5	DPREHEAT	BPIPE10	GMTURB	GBFW
GBFW	OR	BPIPE11	DPUMP2			
GMTURB	OR	GTURBOUT	BPIPE12	BEJ11		
GDEAIR	OR	BPIPE20	BEJ10	DDEAIR	DPOLISH	GPOLISH
GCONSF	OR	BPIPE6	DDRUM	GLPAIR		
GTURBOUT	OR	BPIPE13	DTURB2	BEJ12	GBOILER	
GPOLISH	AND	DMKUP	DNH3.2			
GLPAIR	OR	BEJ15	DLPAIR	BPIPE17	GPTURB	
GBOILER	OR	BVALV	DBOILER2	DBOILER1	BPIPE14	BEJ13
GPTURB	OR	BEJ16	BPIPE8	DTURB		

Table 1 Fault Tree (text format)

Above table shows events also besides the gates. The events starting with a 'B' imply basic events which don't have further explanations e.g. the faults in pipe lines and expansion joints. Others which start with a 'D' imply failures in the designs of the components.

After describing the reliability data for each event in the RDB module one proceeds to the Fault Tree Analyzer module. Here some parameters have to be specified to run the program for cut set analysis. First of all , it asked about the maximum order for the cut sets . It was taken as 10 because it could be visualized ,by looking at the tree (having only 2 AND gates), that the maximum order of cut sets could not be more than this. Next requirement was for the truncation cut off probability. It was tried to be fixed it at the lowest value possible (to have an idea about all the cut sets) and this was 1×10^{-30} with the given computer. It also asked about the method of processing and the mixed

approach (other two options being - bottom - up & top - down) has been followed. The results obtained are as following -

5.1. Operational Unavailability

The unavailability figure was obtained as 0.0011 per hour, which implies approximately 10 failures per year.

5.2. Cut Sets - Analysis & Numbers

The list of minimal cut sets obtained by the analysis is put on the next page. They are total 48 in number.

The number of cut sets of order 1 is 40, of order 2 is 7 and of order 3 is 1. Most of the cut sets have only one element(40 out of 47). When the failure events are connected by OR gates it means that even the occurrence of any one of the failure events causes failure at the top. As apparent from the fault tree, the total number of gates is 21. The number of OR gates is 19 and AND gates are only 2. Even these two AND gates appear at the lower echelons of the tree (first AND gate appearing at water exchanger supply failure which comes at the fifth step of the tree, from its top). This explains the reason behind such a large number of cut sets with only a single element in them.

For explanation of the value of average unavailability which is at 0.0011, an order of magnitude more than the highest failure rate of a single basic event i.e. the boiler at 0.000228, once again the fault tree structure with 19 OR gates assumes significance. Since the individual probabilities are added when events are connected by OR gates, it results in a large unavailability value (where as with the AND gates , they get multiplied).

LIST OF CUT SETS

No.	Probability of failure	Components			
1	2.280000e-004	DBOILER2			
2	2.280000e-004	DBOILER1			
3	1.140000e-004	BVALV			
4	1.140000e-004	DPUMP2			
5	1.000000e-004	DTURB			
6	1.000000e-004	DTURB2			
7	2.280000e-005	DSAT			
8	1.800000e-005	DPUMP			
9	1.140000e-005	DWX			
10	1.140000e-005	DPREHEAT			
11	1.140000e-005	DDRUM			
12	1.140000e-005	DLPAIR			
13	9.400000e-006	BPIPE12			
14	9.400000e-006	BPIPE5			
15	9.400000e-006	BPIPE10			
16	9.400000e-006	BPIPE9			
17	9.400000e-006	DSUP			
18	9.400000e-006	BPIPE4			Cut sets of order 1
19	9.400000e-006	BPIPE8			
20	9.400000e-006	BPIPE3			
21	9.400000e-006	BPIPE14			
22	9.400000e-006	BPIPE11			
23	9.400000e-006	BPIPE17			
24	9.400000e-006	BPIPE2			
25	9.400000e-006	BPIPE13			
26	9.400000e-006	BPIPE6			
27	9.400000e-006	BPIPE1			
28	5.900000e-008	BEJ5			
29	5.900000e-008	BEJ20			
30	5.900000e-008	BEJ14			
31	5.900000e-008	BEJ1			
32	5.900000e-008	BEJ4			
33	5.900000e-008	BEJ16			
34	5.900000e-008	BEJ15			
35	5.900000e-008	BEJ2			
36	5.900000e-008	BEJ11			
37	5.900000e-008	BEJ13			
38	5.900000e-008	BEJ12			
39	5.900000e-008	BEJ7			
40	5.900000e-008	BEJ3			
41	2.052000e-010	DNH3.1	DPUMP3		
42	1.299600e-010	DNH3.1	DPOLISH		
43	1.071600e-010	DNH3.1	BPIPE19		
44	1.071600e-010	DNH3.1	DDEAIR		Cut sets of order 2
45	1.071600e-010	DNH3.1	BPIPE20		
46	6.726001e-013	DNH3.1	BEJ9		
47	6.726001e-013	DNH3.1	BEJ10		
48	1.221624e-015	DNH3.1	DMKUP	DNH3.2	Cut set of order 3

Average Unavailability 0.0011

Chapter 6

SUMMARY AND CONCLUSIONS

An unavailability figure of about 10 failures per year was obtained. According to the Captive Power Plant experience the average plant outage there is about 65 days every year. Actually it is the planned shut down time this year which the Technical Manager, CPP has requested from the Factory Administration [7]. A half of this is constituted by the Annual Statutory Maintenance requirements. The rest of the time is accounted by the troubles in the plant and their correction . These 30 odd days include the repair work also.

The results predict only the expected number of failures, not the overall plant shut down period. This is due to the fact that the repair time data haven't been included for the component failures. It appears that the expected number of failures at 9 per year are a bit more but it should be noted that the by-pass section has not been included in this study, which can provide the required process steam if the boilers are firing and BFW supply is on. Also the personnel at CPP don't consider it as a complete outage when they are supplying a partial output , say 80 TPH instead of 100 TPH of steam, which is indeed a failure in this study.

To get an idea about the relative importance of various components, keeping in view their impact on plant availability, it is needed to once again refer to the list of cut sets on the last page. It shows them in the order of probability. Since a large part of them have single components, failure rate of the components itself appears as the probability of failure for the cut sets. It has been found , as expected , that the two boilers are the two weakest links in the chain of failure events (Actually the Induced Draught Fans and the Ash Conveyors create maximum troubles here). They are followed by the main steam valve and the BFW pump. The two turbines (12 MW and BFW pump's) are the next

along with the saturator. Failure probabilities of various heat exchangers are very small and they are seldom expected to fail. The failure probabilities due to pipes and expansion joints are even lesser.

The cut sets of order more than unity belong to the BFW supply unit i.e. the section containing polisher and deaerator. They have very-very small probabilities of failure as they involve two or more components failing simultaneously.

This analysis can suggest stand by units for boilers, BFW pump and main steam valves. As for the boilers, there is one old Lanchashire Boiler standing besides the new CPP (commissioned in 1983) and the factory actually puts them into operation when both the new boilers are down. The Company is planning to install a new stand by for the BFW pump in near future. The by-pass section takes care of a fault in the main steam valve but then power generation is not there. Thus a stand by for the main steam valve is a necessity.

A further study of the above problem can be suggested where time dependent failure rates would be considered . Then, linearly increasing hazard model seems to be an appropriate one because most of the components in the plant are such that they are exposed to continuous wear. Also, the repair times for various components which fail can be incorporated in the analysis and thus total expected outage time in an year can be estimated . One can also consider the plant in full details i.e. instrumentation, elaborated piping , controls and other equipments, which don't come in a steam balance diagram. The unavailability figure coming out of such a study may be expected to be nearer to the reality.

REFERENCES

1. Srinath, L. S., "*Reliability Engineering*", East West Press, New Delhi, 1991.
2. Fussel, J. B., Henry, E. B. and Marshall, N. H., "MOCUS - A Computer Program to Obtain Minimal Cut Sets from Fault Trees", *ANCR* - 1156, 1974.
3. Chatterjee, P., "Fault Tree Analysis: Reliability Theory and Systems Safety Analysis", *ORC* 74 - 34, University of California, Berkeley, 1974.
4. Draft Manual, PSAPACK 4.2, IAEA, Vienna, 1993.
5. Singh, K. K., "*Generalized Fault Tree Analysis for Reactor Safety* ", M. Tech. Thesis, I.I.T. Kanpur, August 1988.
6. Heneley, E. J. and Kumamoto, H., "*Reliability Engineering and Risk Assessment*", Prentice Hall, 1981.
7. Ray, S., Technical Manager, Captive Power Plant, Duncan Industries Ltd., Kanpur, "Personal Communications", Dec. 1995 - March 1996.
8. IAEA - GRDB Library, RDB Module, PSAPACK 4.2, Vienna, 1993.

122029

Date Slip

This book is to be returned on the date last stamped.

122029

ME-1996-M-MAL-REL

A122029